Smart Grid Industrial Control System Baseline Procurement Guidance

This document provides cyber security procurement language for acquisition of Utility Control Systems (UCS) (i.e. Supervisory and Data Acquisition [SCADA]), Building Control Systems (BCS) (i.e. Direct Digital Control [DDC]), Advanced Meter Infrastructure (AMI) and Utility Monitoring Control Systems (UMCS). The intent of this document is to provide cyber security requirements that can be inserted into Statements of Work that involve the procurement, installation, and verification of secure operation of Industrial Control System (ICS) assets.

1. INSERT INTO SCOPE OF WORK SECTION

This ICS infrastructure shall be authorized under the Department of Navy Risk Management Framework (RMF) for DoD Process per the most current versions of the following Standards and Regulations:

- DoDI 8500.01, Cybersecurity
- DoD Instruction 8510.01, DoD Risk Management Framework (RMF) for DoD Information Technology (IT).
- NIST SP 800-37 (The Risk Management Framework)
- NIST SP 800-82 (Guide to Industrial Control Systems (ICS) Security)
- NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)

Current guidance available at:

- [https://www.dadms.navy.mil](https://www.dadms.navy.mil)
- [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)

Legacy devices that are not required in the new system configuration shall be disconnected, removed and turned over to the government. All provided equipment and software shall be currently marketed products, not currently scheduled for end of life or obsolescence, to ensure system sustainability. Network hardware and software products should have been evaluated and accredited at a licensed/approved evaluation facility and listed as being in conformance to the Common Criteria for IT Security Evaluation (ISO Standard 15408, visit [https://www.niap-ccdev.org](https://www.niap-ccdev.org) for more information). Operating systems and malware/antivirus protection application(s) must also be approved for use by the Department of the Navy in the DoN Applications and Database Management System ([https://www.dadms.navy.mil](https://www.dadms.navy.mil)). All software licenses are required to be in the name of the Department of the Navy.

2. INSERT INTO DOCUMENTATION SECTION

All documentation shall be submitted in the form of five (5) sets of CD-ROM containing native (editable) file formats. All software licenses are required to be in the name of the Department of the Navy.

Security Controls documents
As part of the 60% and 100% design submittal, provide the following document deliverables:

System Authorization Documents
a) Draft hardware list (Hardware list must include the following for each device):
   - Manufacturer,
   - Model,
   - Location,
   - key technical ratings (e.g. memory),
- Serial number,
- MAC addresses,
- IP addresses.

b) Software List (Software list must include the following for each device):
   - Manufacturer
   - Version/subversion,
   - Location/device,
   - Used network ports/protocols/services.

   (Both hardware and software lists should also include Common Criteria EAL status, DADMS entry number, and OS/IOS/Firmware version(s) as applicable).

c) Network diagram
   - Network diagram must show equipment locations, names, models, and IP addresses on network communications schematic.

**Access Controls Summary**

a) Information on software access controls, port control, and protection.

b) System user roles implemented by application and access privileges assigned by default to each role. If privileges can be added to, or removed from, a role, so specify.

c) Details on system logon, including denial after three (3) invalid attempts, how to delay subsequent logons.

d) Details on privileged accounts - who should have them and when are they used.

e) Details on kinds of accounts, their associated privileges, which roles should have access, and so on - servers, wireless, equipment, meters.

f) User ID/Password requirements and/or PKI requirements including details on shadowing, enforcement of password strength, encryption of passwords.

g) Details of system library structure and what roles should be allowed what access privileges to library components.

h) Details on remote (wireless) access by laptops or servers to meter and/or radio data.

**Auditing Controls Summary**

Details on auditing controls and auditing (creation of system audit trail for user accountability).

**Configuration Management Plan**

a) Vendor configuration management plan.

b) Information required to test all patches and upgrades prior to deployment, including coordination as required with any test procedures run at vendor labs.

**Contingency Plan**

a) Restoration Procedures – Guidance on restoring vendor software & hardware including guidance to help determine priority for restoration.

b) Startup & Shutdown Procedures – Details of system initialization, shutdown/aborts designed to ensure secure system state.

**Security Features Guide**

a) List and discussion of all security features of Vendor hardware and software.

b) Document use of mobile code (e.g. scripts, such as Java) and protections in place to prevent malicious content from using associated runtime systems.

c) Documented FIPS 140-2 validated cryptography (or equivalent) compliance.

**Vulnerability Management Plan**

a) Information required to test all patches and upgrades prior to deployment, including coordination as required with any test procedures run at vendor labs.

b) Security issues associated with implementation and maintenance of the application.

c) Cybersecurity POC for resolution of Cybersecurity issues post accreditation.
Maintenance Plan  
  a) Names and other required information of personnel who will be authorized to perform maintenance in accordance with maintenance agreement

Documented Statements  
  a) Declaration that public domain software (e.g., freeware, shareware) is not used in the system.
  b) Information on Common Criteria or National Information Assurance Partnership (NIAP) or Federal Information Processing Standards (FIPS) evaluation status of hardware and software.

3. INSERT INTO CLOSE OUT DOCUMENTATION SECTION

Include the following documents:

- As-built System Accreditation Documents (Security Controls documents, along with as-built drawings submittals). Follow requirements for as-built drawings submittal format, and additionally provide hardware and software lists in Microsoft Excel 2010 or .cvs format and the network diagram in editable AutoCAD 2010 format.

- Request an editable version of the NAVFAC ICS Checklist from the government, and annotate with information required by the checklist, as well as the date and name of the government representative who witnessed validation of each item. (Demonstrate to the satisfaction of the government that system components are in compliance with the NAVFAC ICS Checklist and Security Controls documentation prior to commissioning. Facilitate government testing of the system via network scans and Security Template Implementation Guide (STIG) testing, and provide support for interpreting scan and STIG test results as needed).

- Complete ICS Inventory (to include the following attributes, in tabular format):

<table>
<thead>
<tr>
<th>General Information</th>
<th>Location Information</th>
<th>Hardware Details</th>
<th>Operating System and Platform</th>
<th>Network Information (Actual Function, not potential function)</th>
<th>Miscellaneous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Assigned Unique ID</td>
<td>Facility Name</td>
<td>Device Type</td>
<td>Embedded OS (Yes / No)</td>
<td>MAC Address(es)</td>
<td>Custodian Name</td>
</tr>
<tr>
<td>Barcode or Identifier</td>
<td>NFAID</td>
<td>Device Sub-Type</td>
<td>OS Vendor</td>
<td>IP Address(es)</td>
<td>Comments</td>
</tr>
<tr>
<td>Region</td>
<td>Commodity</td>
<td>Device Function</td>
<td>Operating System (O/S)</td>
<td>Upstream Device</td>
<td>Custodian Organization</td>
</tr>
<tr>
<td>Installation</td>
<td>Floor</td>
<td>Manufacturer</td>
<td>O/S Version</td>
<td>Protocols In Use</td>
<td>Custodian Phone</td>
</tr>
<tr>
<td>Special Area (Option DNAl)</td>
<td>Room</td>
<td>Product Line</td>
<td>Platform Vendor</td>
<td>Host Name</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Model #</td>
<td>Platform Product Line</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Type</td>
<td>Serial #</td>
<td>Platform</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functional System or Equipment Control</td>
<td>Remote Connectivity: (Wired / Wireless / None)</td>
<td>Platform Version</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Type Used: (Serial / Ethernet / Both / None)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For every PLC, RTU, Supervisory Controller, or other network-capable (whether networked or not upon delivery) control device, delivered on CD/DVD:

- Original firmware
- Original firmware hash
- SOP for application of firmware updates/patches
- POC or website for firmware updates/patches
- Count of interfaces and types
- Protocols in use, per interface
- Configuration file
- SOP for configuration